可信计算在区块链行业中的应用及投资逻辑

Frank 李硕淼

1 什么是可信计算

可信计算（Trusted Computing）可以定义为“在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。”[1]. 早期可信计算的发展主要是以TCG（国际可信计算工作组）组织为主。

1.1 可信计算核心技术

可信计算是一个由多种计算机相关技术组合而成的，其实有5个技术概念是可信计算的核心：

1. Endorsement key 签注密钥，签注密钥是一个2048位的RSA公共和私有密钥对，它在芯片出厂时随机生成并且不能改变。这个私有密钥永远在芯片里，而公共密钥用来认证及加密发送到该芯片的敏感数据
2. Secure input and output 安全输入输出 安全输入输出是指电脑用户和他们认为与之交互的软件间受保护的路径。当前，电脑系统上恶意软件有许多方式来拦截用户和软件进程间传送的数据。例如键盘监听和截屏。
3. Memory curtaining 储存器屏蔽 储存器屏蔽拓展了一般的储存保护技术，提供了完全独立的储存区域。例如，包含密钥的位置。即使操作系统自身也没有被屏蔽储存的完全访问权限，所以入侵者即便控制了操作系统信息也是安全的。
4. Sealed storage 密封存储 密封存储通过把私有信息和使用的软硬件平台配置信息捆绑在一起来保护私有信息。意味着该数据只能在相同的软硬件组合环境下读取。例如，某个用户在他们的电脑上保存一首歌曲，而他们的电脑没有播放这首歌的许可证，他们就不能播放这首歌。
5. Remote attestation 远程认证 远程认证准许用户电脑上的改变被授权方感知。例如，软件公司可以避免用户干扰他们的软件以规避技术保护措施。它通过让硬件生成当前软件的证明书。随后电脑将这个证明书传送给远程被授权方来显

示该软件公司的软件尚未被干扰（尝试破解）。
这5个关键技术是一个完备的可信计算系统所应该拥有的。

1.2 可信计算发展

可信计算最初期发展方向为 TPM 硬件芯片。TPM 全称为 Trusted Platform Modular（可信赖平台模块），是可信计算领域的规范标准。此规范由可信赖计算组织（Trusted Computing Group，TCG）制定。 TCG 的前身为信赖运算平台联盟（Trusted Computing Platform Alliance，TCPA）,于 1999 年 10 月份由多家 IT 巨头联合发起成立，初期加入者有康柏、HP 、IBM、Intel、微软等，该联盟致力于促成新一代具有安全且可信赖的硬件运算平台。2003 年 3 月，TCPA 增加了诺基亚 、索尼等厂家的加入，并改组为可信赖计算组织（Trusted Computing Group，TCG），该组织希望从跨平台和操作环境的硬件和软件两方面，制定可信赖电脑相关标准和规范，因此提出了 TPM 规范。其中 TPM1.2 规范比较经典，大多数厂家的芯片都以 TMP1.2 为标准，该规范现已经升级到 2.0，也称之为“Trusted Platform Module Library Specification” [2]。

随着可信计算的发展，可信计算的研究方向已经由传统硬件芯片模式转向了可信执行环境（TEE, Trusted Execution Environment）这种更容易被广泛应用的模式，基于 Intel 芯片的 SGX 以及基于 ARM 开源框架的 TrustZone 是可信执行环境中最被广泛认知且应用的。

1.3 TPM 安全芯片、SGX 及 TrustZone

1.3.1 TPM 安全芯片

TPM安全芯片是指符合TPM（可信赖平台模块）标准的安全芯片，它能有效的保护PC，防止非法用户访问。安全芯片主要是针对商业用户，需要配合软件进行使用。主要拥有下列几个应用场景

1. 存储、管理 BIOS 开机密码以及硬盘密码：将密钥存储于固化在芯片的存储单元中，使其安全性要大为提高。
2. TPM 安全芯片可以进行范围较广的加密：除了开机密码，硬盘密码的储存，用户也可以将应用软件密码存入芯片当中。
3. 加密硬盘的任意分区：配合软件可以在加密硬盘中的任意一部分，并将敏感数据存入其中。电脑的备份恢复功能是该功能的一种应用。

1.3.2 Intel SGX

Intel SGX 全称 Intel Software Guard Extensions，是对因特尔体系（IA）的一个扩展，用于增强软件的安全性。将合法软件的安全操作封装在 enclaves（飞地）中，保护其不受恶意软件的攻击，特权或者非特权的软件都无法访问 enclaves，也就是说，一旦软件和数据位于容器中，即便操作系统或者和 VMM（Hypervisor）被攻破，也无法影响容器里面的代码和数据。一个 CPU 中可以有多个安全 enclaves。

Intel SGX 的最大优势在于其只信任自己和 Intel CPU，此机制将 SGX 的可信级别提高到了硬件级别。软件层面的攻击甚至操作系统层级的攻击都无法威胁到 SGX 创造的可信环境。此架构很利于用户使用目前基于多租户云服务架构下的软件，因

为即使黑客通过云端植入向 PC 控制底层操作系统（OS），因为 SGX 只信任自己和 Intel CPU 的属性，也无法操纵底层操作系统对 SGX 进行攻击。目前，Intel 在 6 代酷睿处理器之后全部配备了 SGX 可信环境。

1.3.3 ARM TrustZone

相对于基于 Intel 系统特有的可信计算环境 SGX，TrustZone 是 ARM 处理器所特有的安全计算环境。不同于 Intel SGX 可以生成多个完全封装的 enclaves，TrustZone 将一个 CPU 划分为两个平行且隔离的处理环境，一个为普通运行环境，另一个为可信运行环境。因为两个环境被隔离，所以很难跨环境操作代码及资源。同时在程序想要进入可信运行环境中时，需要执行安全监控中断指令，让操作系统检查其安全性只有通过检验的程序才能进入安全区。此机制确保了 TrustZone 的安全性，但也意味着整个系统的安全性由底层操作系统（OS）来全权负责。

随着ARM芯片的普及，TrustZone可信环境获得了更加广泛的应用。目前应用主要集中在机顶盒、车载设备以及最常见的智能手机尤其是配备Android系统的。例如高通的Qcomsee、三星的Trustonic以及Google的Trusty。苹果的IOS是个特例，因为他虽然使用ARM处理器，但是不使用TrustZone。而是使用自己研发的类似于Intel SGX机制的Secure Enclave（安全飞地）来处理其安全相关的任务。

1.3.4 SGX 与 TrustZone 的差异

比较SGX和TrustZone，两种安全环境还是有些不同的。主要表现为以下几点：

1. SGX是Intel处理器中的可信环境，TrustZone为ARM处理器中的可信环境。两个应用场景存在不同，Intel主要为PC而ARM主要为手机、机顶盒等小型移动设备。

2. SGX的理论安全性相对于TrustZone更高，因为SGX的安全威胁处于操作系统下的硬件层，而TrustZone的安全威胁可以来自于操作系统层。
3. 一个Intel CPU中可以存在多enclaves可信环境，而TrustZone不同，只有两个环境分别为普通环境以及安全环境。
4. 使用TrustZone，开发难度相对来说较小。因为其本质为将可信资源与非可信资源在硬件上实现隔离。而SGX不同，开发者需要重构代码。虽然Intel提供了SGX的SDK来协助对接，但是对接的工作量依然很大，因此由于开发造成的安全问题是SGX开发者需要面对的一个大问题。

1.4 SGX 面临的问题

对方的负担

1. SGX是一个高度中心化的技术，其内嵌于Intel芯片，同时也是Intel公司的一项商用产品。这就意味着如果Intel芯片或其服务器出现问题， 或者Intel关闭此项功能，将会影响到SGX的使用， 基于其所做的项目将无法运转。
2. 同时因为SGX被Intel所控制，如果想将SGX进行商用，节点使用SGX是需要同Intel签署协议并付费，同时需要基于SDK进行大量的代码开发，这样使SGX的使用成本较高。
3. SGX虽然同其他技术相比比较快，但效率仍然很难满足大规模的商业应用。因为CPU本身的空间较小，而且因为SGX在硬件层，意味着pages在进入以及离开硬盘的时候都需要进行加密，因此运行速度还是比较慢的，并且提速的难度较大。
4. SGX到目前为止已经爆发过两个较大的漏洞。

   (1)第一个是SgxSpectre攻击，SgxSpectre是典型的侧道攻击（侧道攻击是指在电子设备运行过程中，通过其时间消耗，电磁辐射等附加信息泄漏而对其攻击，这类攻击的有效性远高于密码分析的数学方法）。这类攻击之所以出现是因为软件库中存在的具体代码模式允许开发人员在应用中添加SGX支持，攻击者可以通过在SGX的SDK中引入重复性代码执行，并在执行中不断查看缓存的大小变化来去进行攻击。研究人员指出“SgxSpectre攻击完全能攻破SGX封装的机密

性，由于存在易受攻击的代码模式并难以清除，因此攻击者可以发动针对任意封装程序的攻击”，此种攻击是非常有效的。Intel目前已经进行补丁修复但难以完全解决。

⑵第二个是近期爆出来Foreshadow漏斗，Foreshadow的漏洞的原理在于虽然病毒无法攻破SGX的防护，但是可以控制除SGX以外的信息，以及SGX与外界的信息交互。在这种情况下病毒可以创建一个虚假的SGX环境，同时病毒可以使其控制的环境相信其伪造环境为真实的，这样之后所有本该进入SGX处理的进程，将会进入由病毒创建的虚假环境。通过这种方式，攻击者可以达到攻击目的并获得隐私信息。Intel目前正在研究此种漏洞，并试图发行补丁，解决此问题。

2 区块链与可信计算

可信计算保护数据隐私性的属性，使其变为区块链技术生态中的重要一环。可信计算相关技术目前多与分布式计算类项目、数据类项目以及layer2链下解决方案相结合。目前，此类项目的关注重点多在于PC端CPU，因此SGX在区块链领域相比于TrustZone，应用更加广泛。后文中，SGX将被作为重点进行分析。

2.1 SGX 类似技术

在区块链相关生态中，与SGX相类似的技术还有如下三个。

1. 同态加密（Homomorphic encryption）

   同态加密的概念由Rivest等人在20世纪70年代首先提出，同态加密是指经过同态加密的数据进行运算得到一个结果，将结果进行解密，可以得到的与同一方法处理未加密的原始数据所得到的结果相同的密码学技术。同态加密又分加法同态、乘法同态以及全同态加密。全同态加密直到2009年才由Craig Gentry提出。

2. 安全多方计算（multi party computation）

   安全多方计算由我国唯一图灵奖得主姚期智院士提出，其提出场景为百万富翁问题暨“在没有可信第三方的前提下，两个百万富翁如何在不泄漏自己真实财产的状态下比较谁更有钱”。及多个持有私有数据的参与方，共同执行一个计算逻辑并获得计算结果。但在过程中，参与的每一方均不泄漏各自数据的计算。

3. 零知识证明（zero knowledge prove）。

   零知识证明，是由S.Goldwasser、S.Micall及C.Rackoff在20世纪80年代初提出的。它指的是证明着能够在不向验证者提供任何有用的信息的情况下，是验证者相信某个论断是正确的。去数学证明不同，零知识证明是概率证明，也就是说可能会存在小概率的误差。

2.2 各类技术的应用

在目前区块链行业的发展中，SGX和零知识证明被较为广泛的应用。同态加密和安全多方计算因为其技术本身的难度较大且效率较低，现阶段很难在真实的应用场景中落地。而SGX和零知识证明已经与区块链技术相结合，下面分别列举使用这两个技术的代表性项目：

1. SGX相关的区块链项目在2018年5月份之后如雨后春笋般冒出，大多数项目落地的场景为分布式计算、AI等方向。Covalent(简称Cova)为其中较早提出使用SGX技术的，Cova想要通过区块链以及SGX技术来解决传统AI、ML（机器学习）领域training（训练）的问题。 在AI领域，一个成熟的算法模型需要使用大量数据的训练。但是许多数据因为其本身私密性较强且价值巨大，无法直接提供给第三方用来训练算法模型。所以造成了算法模型拥有方有强烈的数据使用需求却无法获得有效数据，而数据持有方想要将数据进行变现却也因为数据的隐私性而无法交易数据。而且常常大型的研究机构既是算法模型拥有方又是数据持有方。在这样的背景下，Cova项目专注于解决在保证数据隐私性的前提下让

数据流通的难题。Cova提供的解决方案是通过区块链和SGX来解决目前的问题。当数据买卖双方向开始交易时，数据拥有者会给网络发一条信息，网络里的所有节点收到信息后会用SGX生成一个Sandbox（沙盒），这样可证保证沙盒环境同时不被任意一个节点、数据买方和数据卖方的控制，数据买方将需要训练的算法模型放进沙盒环境，同时数据卖方将数据放入沙盒环境当中，并开始进行训练，当训练任务结束后，被训练后的算法模型的参数将返还到买方手中，同时沙盒环境自动销毁，并将销毁过程写进者TEE中。在此过程中，SGX负责生成沙盒，控制沙盒输入输出以及销毁沙盒。这样既保证了数据隐私性，又能使算法模型得到训练，较好的解决了目前的问题。

除了Cova之外，Ankr项目试图使用区块链+TEE（SGX）技术解决分布式计算的问题。Taxa想通过TEE（SGX）来实现智能合约的off-chain（链下）运行，以此来提高可扩展性。

2．使用零知识证明技术的项目中，最出名的为Zcash。Zcash使用零知识证明技术在不向对方提供可以证明身份的秘钥的前提下，还能证明自己的身份。实现此过程，需要被验证身份方回答16次以上的相关问题，如果全部答对才能确认其身份。被验证身份方想要通过猜的方式答对全部16个问题的概率约为1/65536，理论上讲这种可能是非常小的。同时Zcash会自动隐藏区块链交易双方的信息以及交易价值，只有拥有正确查看秘钥的人才能访问，这样更好的保证了交易的隐私性。 但是零知识证明的问题也很明显，每笔交易都需要一系列复杂过程，因此效率较低。

3 总结及个人相关领域投资逻辑

在区块链生态当中，可信计算技术不光拥有同态加密、零知识证明、多方安全计算

等技术所具备的保护数据隐私性的属性，同时可信计算可以保证计算结果是可信的，这是共享算力的基本前提，也是其他技术目前所不具备的。同时SGX的速率与其他密码学解决方案相比也有着很大的优势。但是SGX还不是最好的解决方案，因为收到Intel中心化问题以及芯片本身安全漏洞问题的制约。希望未来可以有效率更高，更安全的解决方案出现。

从投资的角度，个人还是比较看好与可信计算结合的相关区块链项目。可信计算在区块链行业中有较多的结合点，并解决了目前数据和区块链行业面临的一些问题。例如在我们已投的项目中，像Taxa项目想要通过可信环境去运行智能合约，以此提升智能合约的效率。区块链行业存在比较大的效率问题，目前很多区块链项目也在试图解决。但是链上的解决方案包括去中心化交易所的匹配系统都无法实现链上的运行，在这样的环境下，链下解决方案目前可能是比较可行的，而可信计算在链下解决方案中将发挥重大的作用。Ankr项目是通过可信计算来实现分布式计算，以此保证数据的安全，此方案解决了目前云计算无法保证数据隐私性的一大问题。Cova项目更多是一个与数据相关的项目，使用可信计算以及区块链技术去解决目前AI、big data领域的一些数据相关问题。

在细分领域中，个人最看好区块链技术与数据类相结合的项目。Facebook2018年4月的用户泄密事件及10月刚刚发生的5000万用户数据泄漏事件已经把个人信息安全问题摆上了桌面，同时在美国，欧洲等发达国家人们对个人信息隐私性，安全性的追求月越来越高，这正是区块链技术以及可信计算结合所能解决的一大问题。在区块链技术的基础上加入可信计算的技术，使得数据的隐私性及安全性得到了更大的保证。未来30年将会是数据的时代，个人认为可信计算与区块链及数据的结合将会较好的处理未来可能所面临的问题。

对于目前可信计算类项目的投资，个人呈谨慎态度。原因如下：
1. 在2018年7、8月，区块链行业已经爆发了一波可信计算类项目的热潮，较多此类型的项目进入到市场。个人认为，目前市场上已经有几个此类型的头部项目，如果无较大技术创新，可以先观望目前头部项目的落地情况再做进一步投资决策。
2. SGX 是目前可信计算中最火的一项技术，但 SGX 出现两个较大漏洞且存在 Intel

重度中心化的问题，现阶段非常难以解决且具有很大的不确定性及局限性。 如果有其他可信计算的技术创新，或者零知识证明、安全多方计算等技术如果有突破性进展，将会是一个非常好的参与机会。

[1] 侯方勇，周进，王志英,等. 可信计算研究[J]. 计算机应用研究, 2004, 21(12):1-4

[2] 周明天，谭良. 可信计算及其进展[J]. 电子科技大学学报, 2006(s1):116-127.